Ueber die Primteilerzerlegung im Kummerschen Zahlkörper sechsten Grades.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der

Hohen
philosophischen Fakultät der Universität Marburg

vorgelegt von

Aloys Herrmann
aus Friedrichsthal (Saar).

MARBURG
Buchdruckerei von Joh. Hamel
1924.

Ueber die Primteilerzerlegung im Kummerschen Zahlkörper sechsten Grades.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der

Hohen
philosophischen Fakultät der Universität Marburg

vorgelegt von

Aloys Herrmann
aus Friedrichsthal (Saar).

MARBURG
Buchdruckerei von Joh. Hamel
1924.

Angenommen von der philosophischen Fakultät Marburg
am 30. April 1924.

Gedruckt mit Genehmigung der Fakultät.

Referent: Herr Geh. Reg.-Rat Professor Dr. Hensel.

R. UNIV.
BIBLIOTHEEK
LEIDEN

Meinem lieben Bruder Julius
gewidmet!

Einleitung.

Im fünften Teile von Hilberts Zahlbericht werden die Zerlegungsgesetze der Primideale eines Kreiskörpers K (ξ) vom Grade $l-1$ in dem Kummerschen Körper K (ξ, ϑ) vom Grade l ($l-1$), wo $\xi = e^{\frac{2\pi i}{l}}$ und $\vartheta = \sqrt[l]{\mu}$ ist, angegeben und zwar werden sie aus den Eigenschaften eines bestimmten Symbols hergeleitet. Im Anschluß daran hat Frl. Sapolsky in ihrer Dissertation den speziellen Fall $l=3$ durchgeführt. Ich möchte in meiner Arbeit diese Frage nach einer neuen, von Herrn Geheimrat Hensel-Marburg angegebenen Weise, behandeln. Dadurch gestaltet sich nun die ganze Lösung gegenüber den in der Kummerschen Idealtheorie angewandten Methoden und Beweisen sehr einfach. Denn bei dieser neuen Behandlungsweise werden nur Methoden angewandt, die schon aus der elementaren Zahlentheorie prinzipiell bekannt sind. Es stellt sich in der Untersuchung auf eine ganz einfache Weise heraus, daß für den Kummerschen Körper sechsten Grades, der zugleich ein Galois'scher bezw. Galois-Abel'scher ist, nicht alle die im Kummerschen Körper sechsten Grades überhaupt möglichen Fälle der Primteilerzerlegung eintreten. Ich zeige außerdem, welcher Zusammenhang im Falle $l=3$ zwischen dem Hensel'schen reduzierten Legendre'schen Symbol und dem Symbol von Hilbert besteht.

Ueber die Primteilerzerlegung
im
Kummerschen Zahlkörper 6. Grades.

I. Die Zerlegung der rationalen Primzahlen im Kreiskörper K (ρ) und die multiplikative Darstellung der Zahlen von K (ρ).

$$\rho = e^{\frac{2\pi i}{3}} = \frac{-1+\sqrt{-3}}{2}.$$

Wir betrachten im Folgenden die Zahlen des Bereiches, der aus K (1), dem Körper der rationalen Zahlen $\frac{m}{n}$, durch Adjunktion einer Wurzel der Gleichung

$$(1)\quad F(x) = x^2 + 3 = 0$$

entsteht und ein sogenannter Kreiskörper ist. Die Zahlen von $K(\rho) = K(\sqrt{-3})$ sind, wie man unter Zuhilfenahme von Gleichung (1) nachweisen kann, alle in der Form

$$(2)\quad \alpha = a \cdot 1 + b\sqrt{-3}$$

darstellbar, wo a und b dem Körper K (1) angehören. Daher heißt das System $(1, \sqrt{-3})$ eine „Basis" von K (ρ). Dieser Bereich ist ein Zahlenkörper, da Summe, Differenz, Produkt und Quotient (mit einem Nenner $\gtrless 0$) von Zahlen der Gestalt (2) wieder diese Gestalt haben.

Zu jeder Zahl $\alpha = a + b\sqrt{-3}$ gehört eine zu ihr „konjugierte" $\alpha' = a - b\sqrt{-3}$, die ebenfalls $K(\sqrt{-3})$ angehört. Im allgemeinen sind α und α' verschieden (primitive Zahlen!). Nur für $b = 0$ ist $\alpha = \alpha'$. Jede Zahl

α des Körpers genügt einer quadratischen Gleichung mit rationalen Koeffizienten, der sog. Hauptgleichung:

$$g(x) = (x - \alpha)(x - \alpha') = x^2 - (\alpha + \alpha')x + \alpha\alpha'$$

$$\text{wo } s(\alpha) = \alpha + \alpha' = 2a \text{ und}$$

$$n(\alpha) = \alpha\alpha' = a^2 + 3b^2$$

die sog. Spur bezw. Norm von α wiederum K (1) angehören. Insbesondere lautet die Hauptgleichung für die Zahl $\rho = \frac{-1 + \sqrt{-3}}{2}$

$$g(x) = x^2 + x + 1 = 0$$

Die Hauptgleichung ist in K (1) irreduzibel und in $K(\sqrt{-3})$ das Produkt zweier konjugierter Linearfaktoren oder in K (1) reduzibel und das Quadrat eines Linearfaktors, je nachdem α primitiv oder imprimitiv ist.

Sind α_1 und α_2 zwei linear unabhängige Zahlen aus K (ρ), so läßt sich jede Zahl linear und homogen mit Koeffizienten aus K (1) durch α_1 und α_2 ausdrücken, also α_1 und α_2 bilden eine Basis.

Zwei andere Zahlen sind dann und nur dann auch eine Basis, wenn sie aus α_1 und α_2 durch eine Transformation mit von Null verschiedener Determinante hervorgehen.

Es seien α_1 und α_2 zwei beliebige Zahlen aus K (ρ)

$$\alpha_1 = a_1 + b_1\sqrt{-3}$$

$$\alpha_2 = a_2 + b_2\sqrt{-3}$$

und α_1' und α_2' die Konjugierten, also:

$$\alpha_1' = a_1 - b_1\sqrt{-3}$$

$$\alpha_2' = a_2 - b_2\sqrt{-3}$$

dann ist auch der Ausdruck

$$\Delta(\alpha_1, \alpha_2) = \begin{vmatrix} \alpha_1 & \alpha_1' \\ \alpha_2 & \alpha_2' \end{vmatrix}^2 = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}^2 \cdot \begin{vmatrix} 1 & \sqrt{-3} \\ 1 & -\sqrt{-3} \end{vmatrix}^2 =$$

$$-12(a_1 b_2 - b_1 a_2)^2$$

von Bedeutung. Diese rationale Zahl heißt die Diskriminante von α_1 und α_2 und ist dann und nur dann gleich Null, wenn (α_1, α_2) keine Basis bilden.

Wenn α eine beliebige Zahl aus K (ρ) ist, nennen wir α ganz, wenn die Hauptgleichung g (x) = 0 ganze rationale Koeffizienten hat. Wie man leicht zeigt, sind alle und nur die ganzen Zahlen des Körpers durch

$$\left(1, -\frac{1+\sqrt{-3}}{2}\right)$$

das sog. „Fundamentalsystem" mit ganzen Koeffizienten darstellbar. Zwei Zahlen α_1 und α_2 bilden dann und nur dann ein Fundamentalsystem, wenn die Substitutionsdeterminante ± 1 ist. Die Diskriminante des Fundamentalsystems $\left(1, -\frac{1+\sqrt{-3}}{2}\right)$ ist:

$$\begin{vmatrix} 1, & -\frac{1+\sqrt{-3}}{2} \\ 1, & -\frac{1-\sqrt{-3}}{2} \end{vmatrix}^2 = -3.$$

Es sei $\alpha_1 = r_1 + r_2 \frac{-1+\sqrt{-3}}{2}$,

$\alpha_2 = s_1 + s_2 \frac{-1+\sqrt{-3}}{2}$, so folgt daß

$$\Delta(\alpha_1\ \alpha_2) = \begin{vmatrix} r_1 & r_2 \\ s_1 & s_2 \end{vmatrix}^2 \Delta\left(1, \frac{1+\sqrt{-3}}{2}\right) = -3$$

also hat die Diskriminante für alle Fundamentalsysteme denselben Wert: — 3, der die „Körperdiskriminante" heißt.

Die Untersuchung der Zahlen des Körpers K (ρ), zu der wir jetzt übergehen wollen, wird nun dadurch wesentlich vereinfacht, daß wir zu einem zu K ($\sqrt{-3}$) isomorphen Körper übergehen: Dem Kongruenzkörper K (x, mod $x^2 + 3$), der dadurch entsteht, daß man alle mod F (x) $= x^2 + 3$ ganzen Funktionen $\frac{g(x)}{h(x)}$ mit rationalen Koeffizienten mod F (x) betrachtet.

Die Elemente dieses Kongruenzkörpers bilden einen Teilbereich des größeren Bereiches aller mod F (x) ganzen Funktionen mit rationalen p-adischen Koeffizienten. Diesen erweiterten Bereich legen wir bei den folgenden Unter-

suchungen über die Teilbarkeitseigenschaften zu Grunde, da diese dann auch für den Teilbereich geliefert werden.

Ist nun — 3 quadratischer Rest für den Bereich von p, d. h. ist das Legendre'sche Symbol $\left(\frac{-3}{p}\right) = +1$, so zerfällt der Modul F (x) in K (p) in zwei p-adische Linearfaktoren f_1 (x, p) und f_2 (x, p) und der erweiterte Bereich ist nur noch ein Kongruenzring, welcher sich in einfacher Weise auf die zwei p-adischen Kongruenzkörper:

$$K_i (x, p) = K_i (x, p \bmod f_i (x, p)] \quad i = 1, 2$$

aller inbezug auf je ein f_i (x, p) ganzen rationalen Funktionen von x mod f_i (x, p) betrachtet, reduziert. Nach H_I ist jedes Element $\alpha = v (x)$ des Ringes R eindeutig in der Form:

$$\alpha \equiv a_1 1_1 + a_2 1_2 = (a_1 a_2) \bmod F (x)$$

darstellbar, wo allgemein a_i der Kongruenzwert von α im Körper K_i ist und umgekehrt gehört zu jedem System $(a_1 a_2)$ ein einziges Element α des Ringes.

Wir ordnen dementsprechend den Primzahlen, für die $\left(\frac{-3}{p}\right) = +1$ ist, d. h. allen Primzahlen $p = 6n + 1$ zwei Stellen p_1 und p_2 zu, und nennen sie „die zu p gehörigen konjugierten Stellen", und jeder der beiden Stellen einen Primteiler und bezeichnen diesen ebenfalls mit p_1 und p_2. Ist

$$\alpha = p^{h_1} E_1 (p_1) \quad \alpha = p^{h_2} E_2 (p_2)$$

so heißt α genau durch $p_1^{h_1}$ $p_2^{h_2}$ teilbar, wo also der Exponent des Primteilers die p-adische Ordnungszahl des Wertes von α für die betreffende Stelle ist. Es gilt der Satz, daß ein Element des Ringes dann und nur dann ganz ist für den Bereich von p, wenn es sowohl für p_1 als auch für p_2 ganz ist.

Ist $\left(\frac{-3}{p}\right) = -1$, was für die Primzahlen $p = 2$, $6n - 1$ zutrifft, dann ist der betrachtete Bereich ein

Körper. Es gilt dann der fundamentale Satz (Vgl. H_I.): Ein Element ist dann und nur dann ganz oder gebrochen, wenn seine Norm ganz oder gebrochen ist.

Es entsprechen somit alle Teilbarkeitseigenschaften der Elemente des Körpers denen ihrer rationalen p-dischen Normen und umgekehrt.

Unter den ganzen Elementen die keine Einheiten d. h. deren Norm nicht eine p-adische Einheit ist, gibt es mindestens ein Element mit möglichst kleiner Ordnungszahl f. Die unendlich vielen äquivalenten Zahlen $\pi' = \varepsilon\,\pi$ für die dies gilt, nennen wir die Primzahlen. Für eine Primzahl π sind nun zwei Zahlen von besonderer Bedeutung: Die Ordnung e und der Grad f. Der Grad ist definiert durch die Gleichung: $n(\pi) = p^f$ E. Die Ordnung e ergibt sich aus $p = \varepsilon\,\pi^e$, da ja allgemein jedes ganze oder gebrochene Element eindeutig in der Form $\alpha = \varepsilon\,\pi^a$ darstellbar ist. Aus $p^2 = n(p) \sim n(\pi^e) \sim n(\pi)^e \sim (p^f)^e = p^{ef}$ folgt, daß $e \cdot f = 2$ ist. Sobald $e = 2$ ist, verliert demnach die reelle Primzahl p ihren Primzahlcharakter.

Es soll nun angegeben werden, wann dies der Fall ist. Dazu verschaffen wir uns zunächst eine Uebersicht über die ganzen Elemente des Kongruenzkörpers.

Satz: Für ungerades p ist $(1, x)$, für $p = 2$ ist $\left(1, \frac{1+x}{2}\right)$ ein Fundamentalsystem, sodaß in der Form: $c_1 \cdot 1 + c_2\,\xi$ alle und nur die ganzen Elemente des Körpers mit ganzen p-adischen Koeffizienten dargestellt sind.

Der Beweis ist klar: Denn

1) p ungerade.

Hier ist $a + b\,x$ mit ganzem a und b sicher ganz und $\frac{a + b\,x}{p}$ kann nur ganz sein, wenn p Teiler von a und b ist.

2) $p = 2$.

Es ist die Norm $\frac{a^2 + 3\,b^2}{4}$ nur ganz, wenn $a^2 - (-3)\,b^2 \equiv 0 \bmod 4$ ist d. h. $a^2 \equiv b^2 \bmod 4$ ist. Dies ist der

Fall, wenn $a \equiv b \bmod 2$. $a - b$ ist dann immer eine gerade Zahl, also $a - b = 2u$. Ich erhalte so für α:

$$\alpha = \frac{a + b x}{2} = \frac{2u + b(1 + x)}{2} = u + b\frac{1 + x}{2}$$

Auch hier ergeben sich aus einem Fundamentalsystem alle anderen durch eine Substitution, deren Determinante eine p-adische Einheit ist. Die Diskriminanten dieser Fundamentalsysteme unterscheiden sich nur um p-adische Einheiten.

Die Körperdiskriminante Δ_p ist also für
ungrades p: $\Delta_p = -12E$

$$p = 2: \Delta_2 = -3E'$$

Jetzt können wir den Satz beweisen:

Satz. Nur $p = 3$ verliert im Kongruenzkörper seinen Primzahlcharakter.

Wenn $\alpha = c_1 \alpha_1 + c_2 \alpha_2$ eine ganze durch p teilbare Zahl ist, dann ist dies auch die Konjugierte $\alpha' = c_1 \alpha_1' + c_2 \alpha_2'$. Daraus erhält man:

$$c_1(\alpha_1 \alpha_2' - \alpha_2 \alpha_1') \equiv 0 \bmod p$$
$$c_2(\alpha_1 \alpha_2' - \alpha_2 \alpha_1') \equiv 0 \bmod p.$$

1. Ist nun p kein Teiler von Δ, so ist jedenfalls p kein Teiler von $(\alpha_1 \alpha_2' - \alpha_2 \alpha_1')$. Nämlich wäre es der Fall, so folgte, daß p^2 Teiler von Δ wäre oder da $p^2 \sim p$ bezw. p^2 ist, so wäre p ein Teiler von Δ.

In diesem Falle muß also sowohl c_1 als auch c_2 durch p teilbar sein, also auch durch p, da ja $p \sim p$ oder $p^2 \sim p$ ist und das heißt
p ist Teiler von c_1, also p^2 Teiler von c_1^2, p Teiler von c_1^2 also p Teiler von c_1. Entsprechend ergibt sich p als Teiler von c_2. Daraus geht hervor, daß jede Zahl α durch p teilbar ist, d. h.

p verliert seinen Primzahlcharakter nicht.

2. Ist p Diskriminantenteiler, also p/Δ, dann ist,

$$c_1(\alpha_1 \alpha_2' - \alpha_2 \alpha_1') \equiv 0 \bmod p$$
$$c_2(\alpha_1 \alpha_2' - \alpha_2 \alpha_1') \equiv 0 \bmod p \text{ ohne daß } c_1$$

und c_2 durch $\mathfrak{p}$, also auch durch p teilbar sind. Das heißt aber nichts anderes als p verliert seinen Primzahlcharakter.

Für $p = 6n - 1$ ist Δ_p und für $p = 2$ ist Δ_2 eine p-adische Einheit. Nur $p = 3$ kann also zerfallen.

Zusammenfassend können wir also sagen:

$p \sim \mathfrak{p}_1 \mathfrak{p}_2$ für $p = 6n + 1$, $p \sim \mathfrak{p}^2$ für $p = 3$, $p \sim \mathfrak{p}$ für $p = 2, 6n - 1$.

oder anders ausgedrückt:

$p \sim \mathfrak{p}_1 \mathfrak{p}_2$, wenn $p \equiv 1 \bmod 3$

$p \sim \mathfrak{p}^2$, wenn $p = 3$

$p \sim \mathfrak{p}$, wenn $p \equiv -1 \bmod 3$

Die multiplikative Normalform.

Bekanntlich ist die Anzahl der mod π inkongruenten ganzen Zahlen gleich $\sigma = n(\mathfrak{p})$. Demnach kann jede ganze Zahl α in der Form $\alpha = \varepsilon^{(0)} + \pi\,\alpha^{(1)}$ dargestellt werden, wo $\varepsilon^{(0)}$ eine Zahl des Restsystems und $\alpha^{(1)}$ eine ganze Zahl ist. Verfährt man so weiter mit $\alpha^{(1)}$ entsprechend der elementaren Zahlentheorie, so erhält man: $\alpha = \varepsilon^{(0)} + \varepsilon^{(1)}\,\pi + \varepsilon^{(2)}\,\pi^2 + \varepsilon^{(3)}\,\pi^3 + \cdots\cdots + \varepsilon^{(k)}\,\pi^{(k)} + \alpha^{(k+1)}\,\pi^{k+1}$ wo die $\varepsilon^{(i)}$ dem Restsystem angehören und $\alpha^{(k+1)}$ eine ganze Zahl ist. Man kann so jede gebrochene oder ganze Zahl für den Bereich einer Stelle $\mathfrak{p}$ eindeutig als eine nach ganzen Potenzen der zugehörigen Primzahl π fortschreitende unendliche Reihe:

$$\alpha = \varepsilon^{(\alpha)}\,\pi^{\alpha} + \varepsilon^{(\alpha+1)}\,\pi^{\alpha+1} + \ldots\ldots\ldots (\mathfrak{p})$$

darstellen, wo die $\varepsilon^{(i)}$ eindeutig bestimmte Zahlen des Restsystems sind und soweit man will, berechnet werden können. Diese π-adischen Reihen können wir in der abgekürzten Form $\alpha = \varepsilon_0, \varepsilon_1\,\varepsilon_2 \cdots (\mathfrak{p})$ schreiben, wo auch (bei gebrochenen Zahlen!) mehr Stellen vor dem Komma stehen können. Diese Reihen sind entweder rationale p-adische Zahlen ($p \equiv 1 \bmod 3$) oder haben die algebraische Entwicklungszahl π und rationale Koeffizienten ($p = 3$)

oder haben p als Entwicklungszahl und algebraische Koeffizienten ($p \equiv -1 \bmod 3$). Von noch größerer Wichtigkeit als diese sog. additive Darstellung ist, besonders für die folgenden Untersuchungen, die sog. Exponential oder multiplikative Darstellung der Zahlen unseres Körpers.

In der π-adischen Entwicklung gehören die Koeffizienten einem vollständigen Restsystem mod π an. Wegen der Existenz sämtlicher $\sigma - 1 = p^f - 1$ Einheitswurzeln in K (p), (die den $\sigma - 1$ mod p inkongruenten Einheiten $\varepsilon^{(1)} \ldots \varepsilon^{(\sigma-1)}$ mod p kongruent sind,) kann man o, 1, w, $w^2 \cdots w^{\sigma-2}$ als vollständiges Restsystem wählen, wo w eine primitive $p^f - 1^{te}$ Einheitswurzel ist. Es läßt sich demnach jede Zahl α aus K ($\sqrt{-3}$) für den Bereich eines eines Primteilers p in eine Reihe $\alpha = w_\alpha \pi^\alpha + w_{\alpha+1} \pi^{\alpha+1} + \cdots$ (p) entwickeln, wo die Koeffizienten eindeutig bestimmte Potenzen einer primitiven $p^f - t^{ten}$ Einheitswurzel oder Null sind. Es ist also $\alpha = \pi^\alpha w^\beta \eta$, wo η eine sog. Einseinheit ist. Diese Einseinheiten sollen nun möglichst einfach multiplikativ dargestellt werden. Je nach dem Zerfallen von p unterscheiden wir hier die Fälle:
I. $p = 6n + 1$, II. $p = 6n - 1$, III. $p = 3$, IV. $p = 2$.

I. $p = 6n + 1$.

Da jedes α aus K ($\sqrt{-3}$) an einer Stelle p_1 bezw. p_2 einer rationalen p-adischen Zahl gleich ist, haben wir hier einfach $\eta = (1 + p)^\gamma$ also

$$\text{I. } \alpha = p^\alpha w^\beta (1 + p)^\gamma \text{ (p)}$$

die aus der elem. Zahltheorie bekannte Darstellung.

Ehe wir nun zu Behandlung von II. III. IV. übergehen, soll noch allgemeiner auf die Fälle $p \sim p^2$, $p \sim p$ eingegangen werden. (Vgl. $H_{II.}$)

Eine π-adische Einseinheit η kann eindeutig als unend-

liches Produkt: $\eta = \eta_1 \eta_2 \eta_3 \ldots$
dargestellt werden, wo

$$\eta_k = 1 + \varepsilon_k \pi^k + \ldots$$

der Basis $\overset{(k)}{\eta}$ für die Einseinheiten k-Ordnung angehört, die man erhält, wenn ε_k sämtliche σ Zahlen eines vollständigen Restsystems durchläuft und die folgenden ε_λ für jedes k beliebig gewählt werden können.

Im Falle $p \sim p^2$ stellt nun

$$(1 + \pi^k + \ldots\ldots)^{c_k} \quad \text{wo } c_k = 0, 1, 2 \ldots (p-1)$$

im Falle $p \sim p$

$$(1 + 1.\pi^k + \ldots)^{c_k} (1 + \xi \pi^k + \ldots)^{c'_k}$$

wo $c_k, c'_k = 0,1 \ldots (p-1)$ und $(1, \xi)$ ein Fundamentalsystem ist, ein vollständiges System $\overset{(k)}{\eta}$ dar für c_k, $c_k' = 0,1 \ldots (p-1)$

Wir können in der Basis (ξ_1, ξ_2)

$$\xi_1 = (1 + \pi^k + \varepsilon_{k+1} \pi^{k+1} + \ldots),$$

$$\xi_2 = (1 + \xi \pi^k + \ldots)$$

für die Einheit k-Ordnung, die willkürlichen ε_i so als Einseinheiten zusammenfassen, daß

$$\xi_1 = 1 + \pi^k \varepsilon, \quad \xi_2 = 1 + \xi \pi^k \varepsilon'$$

ist, wo $\varepsilon, \varepsilon'$ Einseinheiten bedeuten.

Um nun alle Einseinheiten als Potenzen von möglichst wenigen darzustellen, benutzen wir folgenden Satz, der über den Zusammenhang zwischen den Basissystemen verschiedener Grade Auskunft gibt:

Satz: Erhebt man eine Einseinheit i. Grades in die p^k te Potenz, so erhält man

$$(1 + \xi \pi^i \varepsilon)^{p^k} = 1 + \xi \pi^i p^k \varepsilon' \quad k = 0, 1, 2 \ldots$$

wo ξ dem Fundamentalsystem angehört, ε, ε' Einseinheiten sind und zwar gilt das für:

$p > 3$ für $i = 1, 2, 3 \ldots$
$p = 3$ für $i = 1, 2, 3 \ldots$, wenn $e = 1$
$i = 2, 3, \ldots$, wenn $e = 2$
$p = 2$ für $i = 2, 3 \ldots$, wenn $e = 1$
$i = 3, 4 \ldots$, wenn $e = 2$.

Der induktive Beweis ist folgender:

Für festes i und $k = 0$ ist die Behauptung richtig. Wir nehmen an, der Satz sei bewiesen für irgend ein k und zeigen, daß er gilt für $k + 1$. Es ist

$$(1 + \xi \pi^i \varepsilon)^{p^{k+1}} = \left((1 + \xi \pi^i \varepsilon)^{p^k}\right)^p$$

$$= (1 + \xi \pi^i p^k \varepsilon')^p$$

Hier hat nach Voraussetzung und da $p \sim \pi^e$ ist

$\eta = 1 + \xi \pi^i p^k \varepsilon'$ den Grad $i + k e = j$

Ich bilde η^p:

$$\eta^p = (1 + \xi \pi^i p^k \varepsilon')^p$$

$$= 1 + p \xi \pi^i p^k \varepsilon' + \binom{p}{2} (\xi \pi^i p^k \varepsilon')^2$$

$$+ \ldots + \xi^p \pi^{ip} p^{kp} \varepsilon'^p$$

Die einzelnen Summanden haben die Grade:

$e + j, \quad e + 2j, \ldots e + (p - 1) j, \; pj$

Als Glied niedrigsten Grades kommt nun das vom Grad $e + j$ und pj in Frage. η_1^p ist demnach Einseinkeit $e + j$ bezw. pjten Grades, jenachdem $e + j \lessgtr pj$ ist. Für $e + j = pj$ könnte das Hauptglied von höherem Grade werden. Ist nun $e + j < pj$ dann ist

$\eta^p = 1 + p \xi \pi^i p^k + \ldots$ höhere Potenzen

$= 1 + \xi \pi^i p^{k+1} + \ldots$

d. h. es folgt aus der Relation,

$$(1 + \xi\,\pi^i\,\varepsilon)^{p^k} = 1 + \xi\,\pi^i\,p^k\,\varepsilon' + \ldots,$$

daß $(1 + \xi\,\pi^i\,\varepsilon)^{p^{k+1}} = 1 + \xi'\,\pi^i\,p^{k+1}\,\varepsilon'' + \ldots$ ist.

Da nun $i \geqq 1$, $k \geqq 0$, $e = 1,2$ also

$j = k\,e + i \geqq 1$ ist, so ist unsere

Bedingung $e + j < p\,j$ oder $j > r = \left[\frac{e}{p-1}\right]$

wo $\left[\frac{e}{p-1}\right]$ die größte in dem Bruch $\frac{e}{p-1}$ enthaltene ganze Zahl bedeuten soll, für

1. $p > 3$ $i \geqq 1$
2. $p = 3$ $i \geqq 1$, wenn $e = 1$
   $i \geqq 2$, wenn $e = 2$
3. $p = 2$ $i \geqq 2$, wenn $e = 1$
   $i \geqq 3$, wenn $e = 2$ immer erfüllt. Daß für

$p = 3$, $i = 1$, $e = 2$
$p = 2$, $i = 1$, $e = 1$
$i = 1,2$, $e = 2$ die Bedingung nicht erfüllt ist,

sieht man sofort. Es kann also hier η^p vom Grade pj werden oder von höherem Grade, wenn nämlich das Glied vom Grade $e + j$ und pj sich fortheben.

Wir betrachten daher zunächst den regulären Fall $p > 3$; $p = 6\,n + 1$ ist in I. erledigt. Es bleibt also

II. $p = 6\,n - 1$

Hier ist $p \sim \mathfrak{p}$, also $p = \pi$.

Wir wählen ε und ε' so, daß für jedes k:

$$1 + \pi^k\,\varepsilon = 1 + p^k\,\varepsilon = (1 + p)^{p^{k-1}} \text{ und}$$

$$1 + \xi\,\pi^k\,\varepsilon' = 1 + \xi\,p^k\,\varepsilon' = (1 + \xi\,p)^{p^{k-1}} \text{ wird.}$$

Jede Einseinheit stellt sich dann also dar durch die beiden Einseinheiten: $(1 + p)$, $(1 + \xi\,p)$ und zwar folgendermaßen:

$$\eta = \eta_1\ \eta_2\ \eta_3 \ldots = (1 + p)^{c_0}\ (1 + \xi\ p)^{c_0}$$
$$(1 + p)^{c_1\ p}\ (1 + \xi\ p)^{c'_1\ p} \ldots .$$

Durch Zusammenfassung erhält man:

$$\eta = (1+p)^{c_0 + c_1 p + c_2 p^2 + \cdots}\ (1 + \xi p)^{c'_0 + c'_1 p + c'_2 p^2 + \cdots}$$
$$= (1 + p)^{\gamma}\ (1 + \xi\ p)^{\gamma_1}$$

Für ungerades p war nun aber $(1, \sqrt{-3})$ ein Funtamentalsystem. Es ergibt sich also für jedes α die eindeutige multiplikative Darstellung:

$$\text{II. } \alpha = p^{\alpha}\ w^{\beta}\ (1 + p).^{\gamma}\ (1 + \sqrt{-3}\ p)^{\gamma'}$$
$$= p^{\alpha}\ w^{\beta}\ \eta_1^{\gamma_1}\ \eta_2^{\gamma_2}\ (\mathfrak{p})$$

wo $\eta_1\ \eta_2$ ein Fundamentalsystem für alle Einseinheiten w eine primitive $p^f - 1$ d. h. $p^2 - 1^{te}$ Einheitswurzel $\gamma_1\ \gamma_2$ ganze p-adische Zahlen sind.

III. $p = 3$.

Hier ist $p \sim \mathfrak{p}^2$ die Zerlegung in Primfaktoren, also $e = 2$, $f = 1$.

Die Bedingungsgleichung $j > r$ ist erst von $i = 2$ an erfüllt. Um alle Einseinheiten durch möglichst wenige darzustellen, spalten wir die Einseinheit erster Ordnung zunächst ab und untersuchen die Einheiten zweiter und höherer Ordnung. Von diesen kann man die Einseinheiten ungerader Ordnung darstellen als Potenzen einer Einheit dritter Ordnung, die gerader als Potenzen einer Einseinheit zweiter Ordnung. Wir wählen hier die Einheit ε, die für jedes k selbstverständlich ganz beliebig sein kann so, daß

$$(1)\ 1 + \varepsilon\pi^k = (1 + p)^{p^{\frac{k-2}{2}}} \text{ für } k \equiv 0 \bmod 2$$

$$(2)\ 1 + \varepsilon\pi^k = (1 + \pi^3)^{p^{\frac{k-3}{2}}} \text{ für } k \equiv 1 \bmod 2.$$

Es ist ja:

$$(1)\ (1 + p)^{p^{\frac{k-2}{2}}} = 1 + \pi^2\ p^{\frac{k-2}{2}}\ \varepsilon' = 1 + \pi^k\ \varepsilon''$$

also nur $\varepsilon = \varepsilon''$ anzunehmen.

$$(2)\ (1 + \pi^3)^p \overset{\frac{k-3}{2}}{=} 1 + p^{\frac{k-3}{2}} \pi^3 \varepsilon' = 1 + \pi^{k-3} \pi^3 \varepsilon''$$

$$= 1 + \pi^k \varepsilon''$$

also nur $\varepsilon = \varepsilon''$ zu setzen.

Daraus erhält man der Reihe nach:

$$1 + \varepsilon_2 \pi^2 = (1 + p)^1$$
$$1 + \varepsilon_3 \pi^3 = (1 + \pi^3)^1$$
$$1 + \varepsilon_4 \pi^4 = (1 + p)^p$$
$$1 + \varepsilon_5 \pi^5 = (1 + \pi^3)^p$$
$$1 + \varepsilon_6 \pi^6 = (1 + p)^{p^2}$$
$$1 + \varepsilon_7 \pi^7 = (1 + \pi^3)^{p^2} \text{ u. s. w.}$$

Für eine beliebige Einseinheit zweiter oder höherer Ordnung erhält man danach:

$$\eta_2\ \eta_3\ \eta_4 \ldots = (1 + p)^{c_0}\ (1 + \pi^3)^{c'_0}\ (1 + p)^{c_1 p}\ (1 + \pi^3)^{c'_1 p} \ldots$$
$$= (1 + p)^{\gamma}\ (1 + \pi^3)^{\gamma'}.$$

Jedes Element α hat demnach die Form:

$$\alpha = \pi^{\alpha}\ w^{\beta}\ (1 + \pi)^{\beta'}\ (1 + 3)^{\gamma'_1}\ (1 + 3\pi)^{\gamma'_2}$$

wo w eine primitive $p^f - 1$ d. h. $3^1 - 1 = 2^{te}$ Einheitswurzel ist. In diesem Falle ist nun $x = \sqrt{-3}$ eine Primzahl π, denn $x^2 = -3 = 3\varepsilon$ ist genau durch 3^1 teilbar, d. h. x hat eine Norm von der kleinsten Ordnungszahl 1. Um nun formal auf eine ähnliche Darstellung zu kommen wie im vorigen Falle, wollen wir die Einseinheit erster Ordnung umformen und mit der zweiten Einheitswurzel zusammenfassen.

Setzt man $\rho^2 = \frac{-1-\sqrt{-3}}{2} = -\frac{1+\sqrt{-3}}{2}$, so ist dann

$$-\rho^2 = \frac{1 + \pi\varepsilon}{2} \text{ d. h. } -2\rho^2 = 1 + \pi\varepsilon.$$

Als Kongruenz mod π^2 erhält man dann

$$\rho^2 \equiv 1 + \pi\varepsilon \bmod \pi^2.$$

Es ergibt sich demgemäß folgende Darstellung

$$\alpha = \pi^{\alpha} (-1)^{\overline{\beta}} (\rho^2)^{\beta'} (1+3)^{\gamma_1} (1+3\sqrt{-3})^{\gamma_2}$$

Setzt man schließlich $(-1)^{\overline{\beta}} (\rho^2)^{\beta'} = w^{\beta}$, wo w eine primitive 6. Einheitswurzel ist, so erhält man endgültig die eindeutige Darstellung:

$$\text{III. } \alpha = \pi^{\alpha} w^{\beta} (1+3)^{\gamma_1} (1+3\sqrt{-3})^{\gamma_2}$$
$$= \pi^{\alpha} w^{\beta} \eta_1^{\gamma_1} \eta_2^{\gamma_2}$$

Hier ist also w eine primitive 6. Einheitswurzel
η_1 η_2 sind Einseinheiten 2. und 3. Ordnung.
γ_1 γ_2 sind triadische Zahlen.

Wir haben also formal die Darstellung von II. Es soll nun eine für das folgende wichtige, etwas andere Darstellung für den Fall $p = 3$ angegeben werden. Setzt man nämlich $\lambda = 1 - \rho$, so ist λ eine Primzahl für den Bereich von $K(p) = K(l)$. Demnach können wir als Basis für die multiplikative Darstellung aller Einseinheiten folgende drei Einseinheiten wählen:

$$\eta_0 = 1 - \lambda,\ \eta_1 = 1 - \lambda^2,\ \eta_2 = 1 - \lambda^3.$$

Man erkennt hieraus sofort, daß die Einseinheiten ungrader Ordnung nicht als Potenzen der Einseinheit erster Ordnung dargestellt werden können, da

$$(1-\lambda)^3 = \rho^3 = 1$$

ist, also keine Einseinheit dritter Ordnung darstellt. Deshalb haben wir das Basiselement $(1 - \lambda^3)$ hinzugefügt. Innerhalb K (l) ergibt sich also folgende multiplikative Darstellung:

$$\alpha = \lambda^{\alpha} w^{\beta} (1-\lambda)^{\gamma_1} (1-\lambda^2)^{\gamma_2} (1-\lambda^3)^{\gamma_3} \quad (l)$$

wo w eine primitive $3^1 - 1 = 2^{te}$ Einheitswurzel, $\gamma_1 = 0$, 1, 2 und γ_2 γ_3 ganze triadische Zahlen sind.

IV. $p = 2$.

Es ist hier $p \sim p$ und $\left(1, \frac{1+\sqrt{-3}}{2}\right)$ ein F.-System. Die Bedingung ist von $i = 2$ an erfüllt. Berücksichtigt man II., so erhält man:

$$\alpha = p^{\alpha} \rho^{\overline{\beta}} (1+2)^{\beta'} (1+2^2)^{\gamma_1} (1+\xi 2^2)^{\gamma_2}$$

wo ρ die primitive $2^2 - 1 = 3^{te}$ Einheitswurzel ist. Aendert man die Hauptlogarithmen, nachdem man die Einseinheit 1. Ordnung $1 + 2 = 3$ durch die äquivalente $1 + (-1)\ 2 = -1$ ersetzt hat und faßt man $(-1)^{\beta'}$ und ρ^{β} zusammen, so erhält man hier

$$\text{IV. } \alpha = 2^{\alpha}\ w^{\beta}\ 5^{\gamma_1}\ (1 + 4\ \xi)^{\gamma_2}$$
$$= 2^{\alpha}\ w^{\beta}\ \eta_1^{\gamma_1}\ \eta_2^{\gamma_2}, \text{ wo}$$

w eine primitive 6te Einheitswurzel, γ_i ganze dyadische Zahlen sind. Auch diese Darstellung stimmt formal mit den vorherigen überein.

II. Der Kummersche Zahlkörper sechsten Grades.

Im vorigen Abschnitt wurde der Kreiskörper der dritten Einheitswurzeln definiert. Bedeutet nun A eine ganze Zahl in $K(\rho)$, welche nicht zugleich die dritte Potenz einer Zahl aus $K(\rho)$ ist, dann ist die Gleichung:

$$x^3 - A = 0$$

im Kreiskörper irreduzibel. Im Anfange der Arbeit wurde schon angegeben, daß $(1, \rho)$ in $K(\rho)$ ein Fundamentalsystem ist. Wir dürfen also die ganze Zahl A in der Form

$$A = r_1 + r_2\ \rho$$

annehmen, wo die Konjungierte

$$A' = r_1 + r_2\ \rho^2$$

ist und r_1, r_2 ganzzahlig aus K (1) gewählt sind. Durch Adjunktion irgend einer der drei Wurzeln v, ρ v, ρ^2 v der Gleichung $x^3 - A = 0$ zu $K(\rho)$ erhält man den Körper $K(\rho, v)$ den sog. Kummerschen Körper. Ehe wir nun zur Zerlegung der Primteiler des Kreiskörpers im Kummerschen Körper übergehen, wollen wir auf den so bestimmten Kummerschen Körper noch näher eingehen. Wir schlagen dabei den von Hilbert im Zahlbericht angegebenen Weg ein.

Wir legen den Kreiskörper $K(\rho)$ als Koeffizientenkörper zu Grunde, bilden eine in $K(\rho)$ irreduzibele reine kubische Gleichung $x^3 - A = 0$ und adjungieren die

Wurzeln dieser inbezug auf $K(\rho)$ relativ kubischen Gleichung zum Kreiskörper. Dann stellen wir fest, welchen Bedingungen der Koeffizient A der relativ kubischen Gleichung genügen muß, damit der entstehende Zahlkörper ein Galois- bezw. Galois-Abel'scher ist.

Die drei aus $x^3 - A = 0$ entstehenden relativ konjugierten Zahlkörper dritten Grades über $K(\rho)$ sind:

$$K(\rho, v),\ K(\rho, \rho v),\ K(\rho, \rho^2 v).$$

Da aber die drei relativ konjugierten Wurzeln $v, \rho v, \rho^2 v$ ganze rationale Funktionen von v sind mit Koeffizienten aus $K(\rho)$ folgt, daß diese drei relativ konjugierten Zahlkörper übereinstimmen, also daß $K(\rho, v)$ relativ zu $K(\rho)$ ein Galois'scher Zahlkörper ist. Die Gleichung

$$x^3 - A' = 0$$

liefert, wenn eine Wurzel mit v' bezeichnet wird, entsprechend die drei relativ konjugierten Zahlkörper

$$K(\rho, v'),\ K(\rho, \rho v'),\ K(\rho, \rho^2 v'),$$

die natürlich ebenfalls gleich sind.

Wir gelangen so zu sechs konjugierten Zahlkörpern, von denen zwar je drei, die aber nicht immer alle sechs übereinstimmen. Unser Zahlkörper $K(\rho, v)$ braucht also inbezug auf $K(1)$ kein Galois'scher Zahlkörper zu sein. Er ist ein solcher, wenn v' in ihm vorkommt. Dazu muß v' gewissen, jetzt anzugebenden Bedingungen genügen.

$K(\rho, v)$ ist ein Galois'scher Zahlkörper, wenn v' eine rationale Funktion von v ist mit Koeffizienten aus $K(\rho)$, also

$$v' = a_0 + a_1 v + a_2 v^2$$

und zwar sind a_0, a_1, a_2 Zahlen aus $K(\rho)$, die ganz oder gebrochen sein können, da $(1, v, v^2)$ eine Basis ist, aber kein Fundamentalsystem zu sein braucht. Die relativ konjugierten Größen erhalten wir natürlich dadurch, daß wir v durch seine Konjugierten ersetzen, also eine Relativsubstitution ausführen, die wir mit

$$\tau = (v, \rho v) \text{ und } \tau^2 = (v, \rho^2 v)$$

bezeichnen und durch Anhängen eines Index andeuten wollen. Es ist also:

$$v' = a_0 + a_1 v + a_2 v^2$$
$$v'_\tau = a_0 + a_1 \rho v + a_2 \rho^2 v^2$$
$$v'_{\tau^2} = a_0 + a_1 \rho^2 v + a_2 \rho v^2$$

Entsprechend bezeichnen wir die Substitution $(v', \rho v')$ bezw. $(v', \rho^2 v')$ mit τ' bezw. τ'^2.

Da v ganz ist, also auch v' ganz ist, so genügen diese drei relativ konjugierten Zahlen einer irreduzibelen Gleichung mit ganzzahligen Koeffizienten. v' genügt außerdem der irreduzibelen Gleichung $x^3 - A' = 0$; wir können also die drei Wurzeln dieser Gleichung so schreiben: v', v'_τ, v'_{τ^2}.

Es folgt daraus

1) $s(v') = v' + v'_\tau + v'_{\tau^2} = 0$, also $a_0 = 0$

2) $n(v') = v' v'_\tau v'_{\tau^2} = A' = v'^3$

Also es ist

$$\underbrace{(a_1 v + a_2 v^2)}_{v'} \quad \underbrace{(a_1 \rho v + a_2 \rho^2 v^2)}_{v'_\tau} \quad \underbrace{(a_1 \rho^2 v + a_2 \rho v^2)}_{v'_{\tau^2}}$$
$$= \underbrace{(a_1 v + a_2 v^2)^3}_{v'^3}$$

Nach Division mit v^3 erhält man:

$(a_1 + a_2 v)(a_1 \rho + a_2 \rho^2 v)(a_1 \rho^2 + a_2 \rho v) = (a_1 + a_2 v)^3$

$(a_1^2 \rho - a_1 a_2 v + a_2 \rho^2 v^2)(a_1 \rho^2 + a_2 \rho v) = (a_1 + a_2 v)^3$

$a_1^3 + a_2^3 v^3 = a_1^3 + a_2^3 v^3 + 3 a_1^2 a_2 v + 3 a_1 a_2^2 v^2$

also $3 a_1 a_2 v (a_1 + a_2 v) = 0$

1) $a_1 + a_2 v = 0$ ist ausgeschlossen, da dann ja $v = -\frac{a_1}{a_2}$ entgegen unserer Annahme in $K(\rho)$ vorkäme.

2) Aus $3 a_1 a_2 v = 0$ ergibt sich, daß $a_1 = 0$ oder $a_2 = 0$ d. h. für v' ergeben sich die Werte

a) $v' = a_1 v$

b) $v' = a_2 v^2$

Um nun zu entscheiden, welchem dieser beiden Fälle ein Abel'scher Zahlkörper entspricht, müssen wir die Galois'sche Gruppe $\mathfrak{G}_6$ des Zahlkörpers $K(\rho, v)$ aufstellen.

Wir haben eben schon angegeben, daß $(1, \tau, \tau^2)$, wo $\tau = (v, \rho v)$ und $\tau^2 = (v, \rho^2 v)$ ist, Relativsubstitutionen inbezug auf $K(\rho)$ sind. Entsprechend bezeichnen wir die Substitutionen des Kreiskörpers inbezug auf $K(1)$ mit $(1, \sigma)$, wo $\sigma = (\rho, \rho^2)$ ist. Durch Kombination von $(1, \sigma)$ mit $(1, \tau, \tau^2)$ erhalten wir die gesuchte Gruppe $\mathfrak{G}_6$.

Fall a.

Wenden wir die Substitutionen $1, \tau, \tau^2$ auf die Zahlen von $K(\rho, v)$ an, so heißt das, wir müssen v durch $v, \rho v, \rho^2 v$ ersetzen. Diejenigen Zahlen von $K(\rho, v)$, die gleichzeitig in $K(\rho)$ vorkommen, hängen nicht von v ab, gestatten also diese Substitutionen, dagegen gehen sie durch Anwendung von σ in die konjugierten Zahlen über. Insbesondere geht

$$x^3 - A = 0 \text{ in } x^3 - A' = 0 \text{ über;}$$

d. h. durch Anwendung der Substitution σ gehen die Wurzeln $v, \rho v, \rho^2 v$ abgesehen von der Reihenfolge in $v', \rho v', \rho^2 v'$ über.

Wir wollen nun unter v' diejenige Wurzel von $x^3 - A' = 0$ verstehen, in die v durch σ d. h. durch Ersetzen von ρ durch ρ^2 übergeht. Es geht dann durch Anwendung von σ die Wurzel

$$\rho v \text{ über in } \rho^2 v' \text{ und } \rho^2 v \text{ über in } \rho v'.$$

Wenden wir die Substitution σ zweimal nacheinander an, so bleiben die Zahlen von $K(\rho)$ ungeändert, also auch die Gleichung $x^3 - A = 0$ und infolgedessen auch die Gesamtheit ihrer Wurzeln.

Wir hatten festgesetzt, daß wir unter v' diejenige Wurzel von $x^3 - A' = 0$ verstehen wollen, die aus v durch Anwendung von σ hervorgeht. Verstehen wir unter v etwa die Wurzel $v = \rho^2 \sqrt[3]{A} = \rho^2 \sqrt[3]{a + b\rho}$ so ist also

$$v_\sigma = v' = \rho^4 \sqrt[3]{a + b\rho^2} = \rho \sqrt[3]{a + b\rho^2}$$

Durch abermaliges Ausüben von σ geht v' über in v''

$$v'_\sigma = v_{\sigma^2} = v''$$

Man sieht sofort, daß $v_{\sigma^2} = v'' = v$ ist.

Denn ersetzt man in $v' = \rho \sqrt[3]{a + b\rho_2}\ \rho$ durch ρ^2 so ergibt sich $v'_\sigma = \rho^2 \sqrt[3]{a + b\rho} = v$. Also ist

$$v_{\sigma^2} = v$$

Die gesuchte Gruppe des Galois'schen Zahlkörpers ist

$$\mathfrak{G}_6 = (1, \sigma, \tau, \sigma\tau, \tau^2, \sigma\tau^2).$$

Wir erhalten sie durch Kombination der Substitutionen σ und τ mit der Einschränkung (1) $\sigma^2 = 1$, $\tau^3 = 1$

(2) $\tau\sigma = \sigma\tau^2$, $\tau^2\sigma = \sigma\tau$.

Daß in der Gruppe das kommutative Gesetz nicht gilt, sieht man aus der Anwendung der Substitutionen $\sigma\tau$ und $\tau\sigma$ auf die spezielle Zahl $\Theta = v$.

Es ergibt sich nämlich für $\Theta = v$

$$\Theta_\sigma = v_\sigma = v' = a_1 v, \quad \Theta_{\sigma\tau} = a_1 \rho v = \rho v'$$

$$\Theta_\tau = \rho v, \quad \Theta_{\tau\sigma} = \rho^2 v'. \quad \text{Also } \sigma\tau \gtrless \tau\sigma.$$

Unter der Voraussetzung $v' = a_1 v$ sehen wir also, daß der Galois'sche Zahlkörper kein Abel'scher sein kann, da das kommutative Gesetz in der Galois'schen Gruppe nicht gilt.

Fall b.

Die Relation $v' = a_2 v^2$ geht durch Multiplikation mit v über in $v v' = a_2 A = B$

wo B in $K(\rho)$ liegt, weil a_2 und A Zahlen aus $K(\rho)$ sind und außerdem B ganz ist, weil v und v' ganz sind, also auch ihr Produkt $v v' = B$. Die Ganzzahligkeit von a_2 ist nicht erforderlich hierzu.

Die Substitution σ bewirkt also, daß

$$v_\sigma = v' = \frac{B}{v} \text{ und } v_{\sigma^2} = v \text{ wird.}$$

Ueben wir auf $v_\sigma = \frac{B}{v}$ die Substitution σ noch einmal

aus, dann wird daraus

$$v_{\sigma^2} = \frac{B_\sigma}{v_\sigma}$$

Da nun $v_{\sigma^2} = v$ und $v_\sigma = \frac{B}{v}$ ist folgt

$$v = \frac{B_\sigma \, v}{B} \text{ also } B = B_\sigma$$

Es bleibt also die Zahl B aus K (ρ) durch σ ungeändert, d. h. aber B. ist eine rationale Zahl.

Auch hier ist die Gruppe der Substitutionen

$$G_6 = (1, \sigma, \tau, \sigma\tau, \tau^2, \sigma\tau^2)$$

Wenden wir auf eine Zahl Θ die Substitutionen an, so sehen wir, daß unter der Voraussetzung $v_\sigma = v' = \frac{B}{v}$ die Gruppe kommutativ wird, also

$$\sigma\tau = \tau\sigma, \ \sigma\tau^2 = \tau^2\sigma \text{ ist.}$$

Wir setzen allgemein an für eine Zahl Θ

$$\Theta = (r_1 + r_2\rho) + (r_1' + r_2'\rho)\, v + (r_1'' + r_2''\rho)\, v^2$$

Dann ist $\Theta_\sigma = (r_1 + r_2\rho^2) + (r_1' + r_2'\rho^2)\, v' + (r_1'' + r_2'\rho^2)\, v'^2$

$$\Theta_\tau = (r_1 + r_2\rho) + (r_1' + r_2'\rho)\,\rho v + (r_1'' + r_2''\rho)\,\rho^2 v^2$$

also $\Theta_{\sigma\tau} = (r_1 + r_2\rho^2) + (r_1' + r_2'\rho^2)\,\frac{v'}{\rho} + (r_1'' + r_2''\rho^2)\,\frac{v'^2}{\rho^2}$

da τ die Zahlen von K (ρ) ungeändert läßt und $v' = \frac{B}{v}$ in $\frac{B}{\rho v} = \frac{v'}{\rho}$ überführt.

$$\Theta_{\tau\sigma} = (r_1 + r_2\rho^2) + (r_1' + r_2'\rho^2)\,\rho^2 v' + (r_1'' + r_2''\rho^2)\,\rho\, v'^2$$

da durch σ ρ in ρ^2 und v in v' übergeführt wird. Da aber $\rho^2 = \frac{1}{\rho}$ ist, so folgt $\Theta_{\sigma\tau} = \Theta_{\tau\sigma}$.

Aus $\sigma\tau = \tau\sigma$ ergibt sich sofort, daß auch $\sigma\tau^2 = \tau^2\sigma$ ist. Denn durch Anwendung von τ auf $\tau\sigma$ und $\sigma\tau$ erhält man

$$(\tau\sigma)\,\tau = \sigma\tau^2$$
$$\tau\,(\sigma\tau) = \sigma\tau^2$$
$$\tau\,(\tau\sigma) = \sigma\tau^2 \text{ also } \tau^2\sigma = \sigma\tau^2$$

Im Falle $v_3 = \frac{B}{v}$ ist der Zahlkörper sechsten Grades $K(\rho, v)$ inbezug auf $K(1)$ ein Abel'scher Zahlkörper. Diese Ergebnisse können wir in folgenden Satz zusammenfassen:

Satz. Im Körper der rationalen Zahlen ist der Körper sechsten Grades $K(\rho, v)$ dann und nur dann ein Galois'scher Zahlkörper, wenn die Zahl v' eine der Bedingungen

$$(1)\quad v' = a_1 v$$
$$(2)\quad v' = a_2 v^2$$

erfüllt. Ist die erste Bedingung erfüllt, dann ist notwendig der Zahlkörper 6. Grades ein Galois'scher, aber nicht zugleich Abel'scher Zahlkörper; ist die zweite Bedingung erfüllt dann ist er notwendig ein zugleich Abel'scher Körper.

Den Galois'schen bezw. Galois-Abel'schen Zahlkörper kann man nun nach einer Bemerkung von Herrn Hensel folgendermaßen näher charakterisieren: Die Bedingungen (1) und (2) können dahin ausgesprochen werden, daß $\frac{v}{v'}$ bezw. $v\,v'$ zu $K(\rho)$ gehören oder durch Erheben zur dritten Potenz, daß $\frac{A}{A'}$ bezw. $A\,A'$ dritte Potenzen in $K(\rho)$ sind.

Dieselben schließen sich aus; denn wären beide zugleich erfüllt, so wäre ja auch ihr Produkt A^2 d. h. A selbst eine dritte Potenz, also $x^3 - A$ in $K(\rho)$ zerlegbar.

Ersetzt man im ersten Falle bei der Primzahlzerlegung von A die Primfaktoren $\mathfrak{p}_i$ und $\mathfrak{p}'_i$ jeder reellen Primzahl $p_i = 6n + 1$ erster Art durch $(\mathfrak{p}_i\,\mathfrak{p}'_i) = p_i$ und $\mathfrak{p}_i$ und trennt in der dann sich ergebenden Gleichung:

$$A = \varepsilon^a \lambda^b \Pi \mathfrak{p}_i^{c_i} \Pi \mathfrak{q}_i^{d_i} \Pi \mathfrak{p}_i^{e_i} \quad \varepsilon = \sqrt[6]{1} \quad \lambda = \sqrt[2]{-3}$$

den größten rationalen Faktor R ab, so daß

$A = R\,A_0 \quad A_0 = \varepsilon^a \lambda^b \Pi \mathfrak{p}_i^{e_i}$ also $A_0' = \left(\frac{1}{\varepsilon}\right)^a (-1)^b \lambda^b \Pi \mathfrak{p}'^{e_i}_i$ wird, so muß

$\frac{A}{A'} = \frac{A_0}{A'_0} = \varepsilon^{2a} (-1)^b \Pi \left(\frac{p_i}{\mathfrak{p}'_i}\right)^{e_i}$ ein Kubus, also $a = e_i = 0$,

d. h. 1) $A = R \sqrt{-3}^b$ $(b = 0,1)$ sein.

Ersetzt man im zweiten Falle bei der Zerlegung von A jedes Paar (p_i, p'_i) durch $\left(\left(\frac{p_i}{p'_i}\right), p_i\right)$ so folgt aus der Darstellung $A = \varepsilon^a \lambda^b \Pi\left(\frac{p_i}{p'_i}\right)^{c_i} \Pi p_i^{c'_i} \Pi q_i^{d_i}$,

$$A' = \left(\frac{1}{\varepsilon}\right)^a (-1)^b \lambda^b \Pi\left(\frac{p'_i}{p_i}\right)^{c_i} \Pi p'^{c'_i}_i \Pi q_i^{d_i}$$ daß

$$A A' = (-1)^b \lambda^{2b} \Pi p_i^{c'_i} \Pi q_i^{2 d_i}$$

daß $A A'$ dann und nur dann ein Kubus in $K(\rho)$ ist, wenn $b = c'_i = d_i = 0$, wenn also

2) $A = \varepsilon^a \Pi\left(\frac{p_i}{p'_i}\right)^{c_i}$ ist, wo ε^a eine beliebige sechste Einheitswurzel bedeutet.

Im Falle des Galois'schen Zahlkörpers ist also die Zahl A eine ganze rationale Zahl, die durch drei teilbar sein kann oder das Produkt aus $\sqrt{-3}$ und einer zu drei primen Zahl, also $A = \pm R, +3R, +R\sqrt{-3}$ wo $(R, 3) = 1$ ist.

A muß in diesem Falle von einer Einheit verschieden sein, da dann nach Obigem $A = \pm 1$ sein müßte und diese Annahme nicht zu einem Kummerschen Körper führt.

Im Falle des Galois-Abel'schen Zahlkörpers enthält die Zahl A außer den Einheiten nur Primzahlen erster Art und zwar muß, wenn eine Primzahl erster Art in der ersten Potenz auftritt, die konjugierte in der zweiten Potenz vorkommen.

Auch hier kommt aus demselben Grund wie eben für A der Wert ± 1 nicht in Frage. Jedoch ist A der Werte $\pm \rho, \pm \rho^2$ fähig, da die dadurch erzeugten Zahlkörper vom sechsten Grad und Abelsche Zahlkörper sind, da die Relation $n(A) = A A' = B^3$ erfüllt ist. Nachdem wir nun die Bedingungen, der die Zahl A genügen muß, aufgestellt haben, damit wir zu einem Zahlkörper $K(\rho, v)$

gelangen, soll im nächsten Abschnitt die im Kummerschen Zahlkörper sechsten Grades überhaupt mögliche Primteilerzerlegung der Primteiler von K (ρ) angegeben werden.

III. Die Zerlegung der Primteiler von K (ρ) im Kummerschen Körper K (ρ, M).

Es sei A eine beliebige Zahl des Kreiskörpers K (ρ), die nicht die dritte Potenz einer Zahl aus K (ρ) ist, dann wird durch Adjunktion einer Wurzel der irreduzibelen reinen Gleichung $x^3 - A = 0$ zu K (ρ) der Kummersche Körper K (ρ, M) vom Relativgrade drei über K (ρ) und vom Grade sechs über K (1) konstituiert. Es soll nun angegeben werden, wie der zur reellen Primzahl p gehörige Primteiler $\mathfrak{p}$ in K (ρ, M) weiter zerfällt.

Die Frage nach dieser Zerlegung ist gleichbedeutend mit der, wie die Funktion

$$F(x) = x^3 - A$$

in K ($\mathfrak{p}$), dem Körper der zu $\mathfrak{p}$ gehörigen π-adischen Zahlen in Primfaktoren zerfällt. Ganz analog konnten wir ja die Zerlegung von p in K (ρ) aus dem Zerfallen von $F(x) = x^2 + 3$ in K ($\mathfrak{p}$) erschließen.

Die Zerlegung der Primteiler eines Kreiskörpers im Kummerschen Körper ist in einem Aufsatze von Herrn Hensel allgemein durchgeführt in Crelles Journal Bd. 151 (citiert als $H_{IV.}$). Ich gebe daher nur die Hauptresultate an, spezialisiert für den Fall $l = 3$. Was die genauen Beweise anbetrifft, so sei daher auf jene Arbeit verwiesen.

Wir nehmen A in der multiplikativen Darstellung an:

$$A = \pi^{\alpha}\, \overline{w^{\beta}}\, \eta_1^{\gamma_1}\, \eta_2^{\gamma}\ (\mathfrak{p})$$

Dabei ist: π eine Primzahl in K ($\mathfrak{p}$), die zur reellen Primzahl p gehört,

w eine primitive P. Einheitswurzel und zwar die höchste in K ($\mathfrak{p}$) vorkommende,

$(\eta_1\ \eta_2)$ ein Fundamentalsystem von e . f Elementen.
γ_1, γ_2 rationale p-adische Zahlen.

Die erste wesentliche Vereinfachung erreicht man dadurch, daß man als Modul des Kongruenzbereiches

$$B\ (x,\ p \bmod F\ [x] = x^3 - A)$$

einen neuen Modul $F_1\ (x_1)$ einführt, für welchen A als kubischer Kern angenommen wird, d. h. wir haben nur die Fälle zu unterscheiden, wo die Exponenten in der multiplikativen Darstellung von A mod 3 reduziert sind, also so beschränkt vorausgesetzt werden können, daß

$$\alpha < 3,\ \overline{\beta} < (3,\ P),\ \gamma_i < (3,\ p^\infty) \text{ ist.}$$

Setzt man $P = 3^n L \quad (3,\ L) = 1$ und zerlegt man entsprechend die Einheitswurzel $\overline{w^\beta}$, so sieht man, daß man die Grundgleichung in der Form

$$x^3 = A = \pi^\alpha\ w^\beta\ \eta_1^{\gamma_1}\ \eta_2^{\gamma_2}\ (p)$$

annehmen kann, wo nun w eine primitive 3^nte Einheitswurzel und $\alpha < 3,\ \beta < 3,\ \gamma_i < (3,\ p^\infty)$ ist.

Von dieser Grundgleichung gehen wir aus.

Wir unterscheiden in der Untersuchung die beiden Fälle $p \gtrless 3$ und $p = 3$.

I. $p \gtrless 3$.

In diesem Falle ist p in K (p) selbst eine Primzahl und die entscheidende Gleichung $x^3 - A = F\ (x)$ reduziert sich auf die einfachere

$$x^3 - p^\alpha\ \omega^\beta = 0\ (p)$$

wo $\alpha,\ \beta < 3$ und ω eine primitive 3^nte Einheitswurzel ist. Um nun die Zerlegung von $x^3 - A$ in K (p) angeben zu können, teilen wir die so in Frage kommenden Zahlen $A = p^\alpha\ \omega^\beta$ in die drei Klassen ein;

A) $\alpha = 0,\ \beta = 0$
B) $\alpha > 0,\ \beta$ beliebig
C) $\alpha = 0,\ \beta > 0$

A) Hier ist $\alpha = 0,\ \beta = 0$ also die ursprüngliche Zahl A ist dritter Potenzrest zu p. Die reduzierte Gleichung lautet: $x^3 - 1 = 0\ (p)$
zerfällt also in K (p) in drei rationale Linearfaktoren

$$x^3 - 1 = (x - 1)\ (x - \rho)\ (x - \rho^2)$$

Der Kongruenzbereich B (x, p mod $x^3 - A$) ist nur noch ein Ring, der sich auf drei p-adische Körper abbilden läßt. Entsprechend wird also hier

$$p \sim \mathfrak{P}_1\ \mathfrak{P}_2\ \mathfrak{P}_3$$

B) $\alpha > 0,\ \beta$ beliebig.
Durch Benutzung einer Substitution kann man diesen Fall so vereinfachen, daß $\alpha = 1$, also daß man den Modul in der Form

$$F(x) = x^3 - p\ \omega^{\beta}\ (p)$$

erhält. Diese Eisensteinsche Gleichung ist mod p irreduzibel, also erst recht in K (p). Unser Kongruenzbereich ist also ein Körper. Daß außerdem p seinen Primzahlcharakter verliert, sieht man auch sofort. Denn aus der Gleichung $x^3 - p\ \omega^{\beta} = 0$ folgt ja, daß das primitive Element x den kleinstmöglichen Relativgrad $f_0 = 1$ hat, da

$$n(x) = p^1\ \omega^{\beta}$$

ist. Da das Produkt aus Relativordnung e_0 und Relativgrad f_0 gleich drei ist, folgt $e_0 = 3$, also

$$p \sim \mathfrak{P}_1^{\,3}$$

C) $\alpha = 0,\ \beta > 0$
Auch hier ergibt sich, daß man $\beta = 1$ annehmen, also von der einfacheren Gleichung:

$$x^3 - \omega = 0\ (p)$$

ausgehen kann, wo ω eine primitive 3^nte Einheitswurzel ist. x kommt also als primitive 3^{n+1}te Einheitswurzel in K (p) nicht vor und man sieht leicht, daß die Konju-

gierten zu x, nämlich x^{p^f} und $x^{p^{2f}}$ mod $\mathfrak{P}$ inkongruent, also für den Bereich von $\mathfrak{P}$ verschieden sind. Die Gleichung

$$x^3 - \omega = 0 \ (\mathfrak{p})$$

erweist sich also in K (p) als irreduzibel und es ist demgemäß

$$\mathfrak{p} \sim \mathfrak{P}_1.$$

II. Fall: $p = 3$.

In diesem Falle ist $3 = p \sim \mathfrak{l}^2$ die Zerlegung in Primfaktoren in K (ρ) und wir hatten die multiplikative Darstellung:

$$A = \lambda^{\overline{\alpha}} w^{\overline{\beta}} (1 - \lambda)^{\overline{\gamma_1}} (1 - \lambda^2)^{\overline{\gamma_2}} (1 - \lambda^3)^{\overline{\gamma_3}}$$

in K (l) gefunden. w war eine primitive zweite Einheitswurzel, $\overline{\gamma_1}$ $\overline{\gamma_2}$ $\overline{\gamma_3}$ waren gewöhnliche triadische Zahlen.

Reduzieren wir mod 3, so ergibt sich für A die einfache Form

$$A = \lambda^{\alpha} (1 - \lambda)^{\gamma_1} (1 - \lambda^2)^{\gamma_2} (1 - \lambda^3)^{\gamma_3}$$

wo $\alpha < 3$, $\gamma_i < (3, 3^\infty) = 3$ ist.

Auch hier teilen wir die für A in Frage kommenden Zahlen in drei Klassen, je nachdem

A) $\alpha = 0$, $\gamma_i = 0$

B) $\alpha > 0$, γ_i beliebig

C) $\alpha = 0$, $\gamma_i > 0$

A) Hier sind α, $\gamma_i = 0$, also A ist dritter Potenzrest. Wie in I_A ist der Kongruenzbereich nur noch ein Ring, der der in drei Kernkörper zerlegt wird und es wird

$$\mathfrak{l} \sim \mathfrak{L}_1 \ \mathfrak{L}_2 \ \mathfrak{L}_3$$

B) Es ist $\alpha > 0$, γ_i beliebig.

Wie in I_B läßt sich die Zahl A so reduzieren, daß die entscheidende Gleichung lautet:

$$x^3 - \lambda^1 (1 - \lambda)^{\gamma_1} (1 - \lambda^2)^{\gamma_2} (1 - \lambda^3)^{\gamma_3} = 0 \ (\mathfrak{p})$$

Da λ für K (l) eine Primzahl ist, so haben wir hier eine Eisensteinsche Gleichung, die in K (l) irreduzibel ist. Die Relativnorm

$$n_l(x) = \lambda^1 \eta$$

sagt ferner, daß $f_0 = 1$, also $e_0 = 3$ d. h.

$$l \sim \mathfrak{L}_1^3 \text{ ist.}$$

C) Es ist $\alpha = 0$, $\gamma_i > 0$ und es läßt sich in diesem Falle durch eine geeignete Substitution erreichen, daß A eine Einseinheit k-Grades wird.

$$A = (1 - \lambda^k)(1 - \lambda^{k+1})^{\gamma_{k+1}} \cdots$$

Ist $k = 1, 2$, so existiert im Kongruenzbereich ein primitives Element x', dessen Norm

$$n(x') = \lambda\eta$$

ist, also deren Ordnungszahl den kleinstmöglichen Wert 1 hat, also ist der Relativgrad $f_0 = 1$ d. h. aber p verliert seinen Primzahlcharakter und es ist

$$l \sim \mathfrak{L}_1^3$$

Ist $k = 3$, also $F(x) = x^6 - (1 - \lambda^3)$

so gelangt man durch eine Substitution zu einem Modul $F_1(x_1)$, der es gestattet für eine Wurzel x_0 der Gleichung $F_1(x_1) = 0$ im Oberkörper zu erkennen, daß diese Wurzel mit ihren Konjugierten mod $\mathfrak{L}$ betrachtet inkongruent ist. Der Relativgrad f_0 von $\mathfrak{L}$ ist daher gleich drei und demnach die Relativordnung $e_0 = 1$, also der Primteiler l in $K(p) = K(l)$ ist unzerlegbar

$$l \sim \mathfrak{L}_1$$

Die in allen Fällen angegebene Zerlegung von p und l im Oberkörper dritten Grades können wir nun in einem einfachen Satz zusammenfassen, da sich die Zerfällung der Primteiler direkt aus der multiplikativen Darstellung von A ablesen läßt.

Nach $H_{III.}$ geschieht dies durch Einführung des sog. erweiterten Legendre'schen Symbols. Es ist die Verallgemeinerung des Legendre'schen Zeichens $\left(\frac{a}{p}\right)$ der elemen-

taren Zahlentheorie. Wir stellen nun kurz die Definition des Symbols in der für uns geeigneten Form auf.

Ist $x^3 = A = \pi^{\alpha}\, w^{\beta}\, \eta_1^{\gamma_1} \cdots \eta_u^{\gamma_u}\ (\mathfrak{p})$

die gegebene reine Gleichung, wo w eine primitive $p^f - 1^{te}$ Einheitswurzel ist, $\eta_1 \ldots \eta_u$ eine Basis für alle Einseinheiten, dann ordnen wir A das Symbol

$$\left\{\frac{A}{\mathfrak{p}}\right\}_3 = (a^{\alpha},\ b^{\beta},\ c_1^{\gamma_1} \ldots c_u^{\gamma_u}) = \mathfrak{a}$$

zu und nennen es den Charakter von A für den Exponenten drei und zwar bedeutet

a eine primitive dritte Einheitswurzel $= \rho$

b „ „ $(3,\ p^f - 1)$ „ $= \rho_0$

c_i „ „ $(3,\ p^{\infty})$ „ $= \rho_1$.

In unserem Falle wird dann für $p \gtrless 3$, wo ja $\rho_1^{\gamma_i} = 1$ ist

$$\left\{\frac{A}{\mathfrak{p}}\right\} = (\rho^{\alpha},\ \rho_0^{\beta})$$

für $p = 3$, wo $\varrho_0^{\beta} = 1$, $\varrho_1 = \varrho$

$$\left\{\frac{A}{\mathfrak{p}}\right\} = \left\{\frac{A}{1}\right\} = (\varrho^{\alpha},\ \varrho^{\gamma_1},\ \varrho^{\gamma_2},\ \varrho^{\gamma_3})$$

Im letzten Falle $p = 3$ fassen wir die ersten drei Elemente zu einer einzigen Gruppe zusammen. Unser Symbol enthält also in beiden Fällen je zwei Elementgruppen. Nunmehr definieren wir das sog. reduzierte Legendre'sche Symbol $R\left\{\frac{A}{\mathfrak{p}}\right\}$ (Vgl. $H_{IV.}$). Es werde $R\left\{\frac{A}{\mathfrak{p}}\right\} = \varrho^a$ gesetzt, wenn die erste von 1 verschiedene Einheitswurzel, welche von links nach rechts auftritt, der ersten Elementgruppe in $\left\{\frac{A}{\mathfrak{p}}\right\}$ angehört,

$R\left\{\frac{A}{\mathfrak{p}}\right\} = \varrho^b$, wenn sie der zweiten Gruppe angehört,

$R\left\{\frac{A}{p}\right\} = 1$, wenn alle Elemente gleich 1 sind, also A dritter Potenzrest ist.

Ich stelle nun die Resultate über die Zerfällung von p und l zusammen.

Wir hatten für $\gtrless 3$: für $p = 3$:

A) $\alpha = 0, \beta = 0$ $p \sim \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$ A) $\alpha = 0, \beta = 0$ $p \sim \mathfrak{L}_1 \mathfrak{L}_2 \mathfrak{L}_3$

B) $\alpha > 0$, β bel. $p \sim \mathfrak{P}^3$ B) $\alpha > 0$, γ_i bel. $p \sim \mathfrak{P}_1^3$

C) $\alpha = 0, \beta > 0$ $p \sim \mathfrak{P}$

C) $\alpha = 0, \gamma_i > 0 \lessgtr \begin{matrix} 1)\ k < 3 & p \sim \mathfrak{L}_1^3 \\ 2)\ k = 3 & p \sim \mathfrak{L} \end{matrix}$

Drückt man dies durch das reduzierte Legendre'sche Symbol aus, so sieht man, daß

$p \sim \mathfrak{P}_1 \mathfrak{P}_2 \mathfrak{P}_3$ ist, wenn $R\left\{\frac{A}{p}\right\} = 1$

$p \sim \mathfrak{P}_1^3$, wenn $R\left\{\frac{A}{p}\right\} = \varrho^a$

$p \sim \mathfrak{P}$, wenn $R\left\{\frac{A}{p}\right\} = \varrho^b$ ist.

Die Primteilerzerlegung läßt sich so in folgendem Satze zusammenfassen (vgl. $H_{IV.}$ S. 120):

In dem durch die reine Gleichung $x^3 - A = 0$ definierten Kummer'schen Körper zerfällt ein beliebiger Primteiler p des Kreisteilungskörpers K (ϱ) in drei verschiedene Primdivisoren oder in drei gleiche Primteiler ersten Grades oder er bleibt unzerlegbar, je nachdem das reduzierte Legendre'sche Symbol $R\left\{\frac{A}{p}\right\}$ von A gleich 1, ϱ^a oder ϱ^b ist.

Die Primteiler des Kreisteilungskörpers K (ϱ) hatten wir wiederum in drei Arten eingeteilt. Wir erhalten daher im Ganzen im Zahlkörper K (ϱ, M) neun Fälle. Frl. Sapolsky hat die in Betracht kommenden Fälle auf S. 67 ihrer Arbeit zusammengestellt. In unserer Ausdrucksweise sieht diese Tabelle folgendermaßen aus:

Körper K (ϱ)	Der Körper sechsten Grades K (ϱ, M).	
I.	a) $R\left\{\frac{A}{p}\right\} = \varrho^a$	$p \sim \mathfrak{P}_1^3$
$p \equiv +1 \bmod 3$	b) $R\left\{\frac{A}{p}\right\} = 1$	$p \sim \mathfrak{P}_1\,\mathfrak{P}_2\,\mathfrak{P}_3$
$p \sim p_1\,p_2$	c) $R\left\{\frac{A}{p}\right\} = \varrho^b$	$p \sim \mathfrak{P}_1$
II.	a) $R\left\{\frac{A}{p}\right\} = \varrho^a$	$p \sim \mathfrak{P}_1^3 \sim p$
$p \equiv -1 \bmod 3$	b) $R\left\{\frac{A}{p}\right\} = 1$	$p \sim \mathfrak{P}_1\,\mathfrak{P}_2\,\mathfrak{P}_3$
$p \sim \mathfrak{p}$	c) $R\left\{\frac{A}{p}\right\} = \varrho^b$	$p \sim \mathfrak{P}$
III.	a) $R\left\{\frac{A}{l}\right\} = \varrho^a$	$l \sim \mathfrak{L}_1^3$
$p = 3$	b) $R\left\{\frac{A}{l}\right\} = 1$	$l \sim \mathfrak{L}_1\,\mathfrak{L}_2\,\mathfrak{L}_3$
$p \sim p^2$	c) $R\left\{\frac{A}{l}\right\} = \varrho^b$	$l \sim \mathfrak{L}$

IV. Die Primteilerzerlegung im Galois- bezw. Galois-Abel'schen Zahlkörper K (ϱ, v).

Wir wollen nun dazu übergehen, die im dritten Abschnitt gewonnenen Ergebnisse auf die beiden im zweiten Abschnitt näher charakterisierten Kummerschen Körper sechsten Grades anzuwenden. Unter Zuhilfenahme der im zweiten Abschnitt gefundenen Form von A und der Tabelle auf dieser Seite zeige ich nämlich, daß nicht alle neun Typen der in einem Kummerschen Körper überhaupt möglichen Fälle bei den Körpern auftreten, und zwar fallen beim Galois'schen Körper die Fälle II_c und III_c fort, beim Galois-

Abel'schen Körper kann der Fall II_a nicht auftreten. Wir können und wollen, indem wir dies zeigen, die Zahl A als kubischen Kern voraussetzen.

Fall II_c des Galois'schen Körpers.

Es ist also zu zeigen, daß, wenn $A = R,\ 3\,R,\ R\sqrt{-3}$ wo $(R, 3) = 1$ ist, für die Primzahlen $p \equiv -1 \bmod 3$ für die ja $p \sim \mathfrak{p}$ ist, das reduzierte Legendre'sche Symbol $R\left\{\frac{A}{p}\right\}$ nie den Wert ϱ^b annehmen kann.

Wenn der Wert ϱ^b überhaupt in Frage kommen soll, dann darf A nicht durch $\mathfrak{p}$ teilbar sein, da sonst das Symbol den Wert ϱ^a annimmt. A ist also prim zu $\mathfrak{p}$ vorauszusetzen. Denke ich mir A multiplikativ dargestellt und dann mod $\mathfrak{p}$ betrachtet, dann ist also

$$A \equiv w^{\beta} \bmod \mathfrak{p}$$

wo w eine primitive $p^f - 1^{te}$ Einheitswurzel und $\beta < 3$ ist.

$$A^{\frac{n(\mathfrak{p})-1}{3}} \equiv w^{\beta\frac{n(\mathfrak{p})-1}{3}} \bmod \mathfrak{p}$$

Für $\beta = 0$ ist A kubischer Rest, also für

$$A^{\frac{n(\mathfrak{p})-1}{3}} \equiv 1 \bmod \mathfrak{p}$$

$$\text{ist } R\left\{\frac{A}{p}\right\} = 1.$$

Ich habe also nur noch zu zeigen, daß $A^{\frac{n(\mathfrak{p})-1}{3}} \not\equiv 1 \bmod \mathfrak{p}$ ist, wenn $p = 3n - 1$, $(A, \mathfrak{p}) = 1$ und $A = R,\ 3\,R,\ R\sqrt{-3}$ ist, $(R, 3) = 1$.

Im Falle $p = 2$ wird das Resultat trivial, weil $A^{\frac{n(\mathfrak{p})-1}{3}}$ sicher $\equiv 1 \bmod 2$ ist, da $\frac{n(\mathfrak{p})-1}{3} = 1$ wird und $(A, \mathfrak{p}) = 1$ ist. Wir können daher sofort $p = 6n - 1$ annehmen.

Da A^{2n} für $A = R, 3R, R\sqrt{-3}$ in jedem Falle eine ratioale Zahl ist, so hat man

$$A^{\frac{n(p)-1}{3}} = (A^{\frac{p+1}{3}})^{p-1} = (A^{2n})^{p-1} \equiv 1 \bmod p$$

Damit ist die Unmöglichkeit, daß $R\left\{\frac{A}{p}\right\}$ im Falle II_c den Wert ϱ^b annimmt, vollständig bewiesen.

Fall IIIc.

Das reduzierte Legendre'sche Symbol

$$R\left\{\frac{A}{p}\right\} = (\varrho^{\alpha}, \varrho^{\gamma_1}, \varrho^{\gamma_2}, \varrho^{\gamma_3})$$

ist dann und nur dann ϱ^b, wenn $\alpha = \gamma_1 = \gamma_2 = 0$ $\gamma_3 \gtrless 0$ das heißt, wenn (1) $(A, p) = 1$ ist, da für $(A, p) = p$ $R\left\{\frac{A}{p}\right\} = \varrho^a$ würde und wenn (2) $A \equiv 1 \bmod p^3$, $A \not\equiv 1 \bmod p^4$ ist. Der Beweis von (2) folgt sofort aus der multiplikativen Darstellung von A:

$$A = (1 + \sqrt{-3})^{\gamma_1} (1 + (-3))^{\gamma_2} (1 + \sqrt{-3}^3)^{\gamma_3}$$

wenn man sie nur mod p^2 und mod p^3 betrachtet.

Dies ist in den drei Fällen $A = R, 3R, R\sqrt{-3}$ unmöglich; die beiden letzten scheiden aus, weil dann $(A, p) \neq 1$ und der erste, weil A rational, also stets eine gerade Potenz von p enthält.

Also ist der Fall III_c beim Galois'schen Körper auszuschließen.

Fall II_a des Abel'schen Körpers.

Daß schließlich für den Kummer'schen Körper 6. Grades, der ein Galois-Abel'scher ist, der Fall II_a nicht auftreten kann, sieht man auch sofort aus der multiplikativen Normalform von A. Denn wie im zweiten Abschnitt festgestellt wurde, darf hier A nur Primzahlen erster Art

enthalten, also darf in der multiplikativen Darstellung für $p \equiv -1 \bmod 3$ die π-adische Kernzahl nicht eine Ordnungszahl > 0 besitzen. Also α muß immer Null sein und das heißt aber, das Symbol $R\left(\frac{A}{p}\right)$ kann für $p = 3n - 1$ niemals den Wert ϱ^a annehmen, also der Fall II_a kommt nie vor.

Wir können nun, da wir die Zerlegung der Primzahlen des Kreiskörpers im Kummer'schen Körper kennen, auch auf die Zerlegung der reellen Primzahlen im Körper K (ϱ, v) schließen. Insbesondere sehen wir, daß die rationalen Primzahlen im Kummer'schen Körper sechsten Grades, der zugleich ein Galois'scher ist, alle zerlegt werden.

Ich stelle das Zerfallen der reellen Primzahlen für die beiden charakterisierten Körper sechsten Grades zusammen in einer Tabelle, aus der die Zerlegung der reellen Primzahlen in K (ϱ, v) direkt ersichtlich ist.

I. Das Zerfallen der reellen Primzahlen im Galois'schen Körper K (ϱ, v).

Die Primzahlen von K (1)	Ihr Zerfallen in K (ρ)	Ihr Zerfallen in K (ρ, v)
$p = 3n + 1$	$p \sim \mathfrak{p}_1\, \mathfrak{p}_2$	$p \sim \mathfrak{P}_1^3\, \mathfrak{P}_2^3$ oder $\sim \mathfrak{P}_1\, \mathfrak{P}_2$ oder $\sim \mathfrak{P}_1\, \mathfrak{P}_2\, \mathfrak{P}_3\, \mathfrak{P}_1'\, \mathfrak{P}_2'\, \mathfrak{P}_3'$
$p = 3n - 1$	$p \sim \mathfrak{p}$	$p \sim \mathfrak{P}_1^3$ oder $\sim \mathfrak{P}_1\, \mathfrak{P}_2\, \mathfrak{P}_3$
$p = 3$	$p \sim \mathfrak{p}^2$	$p \sim \mathfrak{P}_1^6$ oder $\mathfrak{P}_1^2\, \mathfrak{P}_2^2\, \mathfrak{P}_3^2$

II. Das Zerfallen der reellen Primzahlen im Galois-Abel'schen Körper K (ϱ, v).

Die Primzahlen von K (1)	Ihr Zerfallen in K (ϱ)	Ihr Zerfallen in K (ϱ, v)
$p = 3n + 1$	$p \sim \mathfrak{p}_1\ \mathfrak{p}_2$	$p \sim \mathfrak{P}_1^3\ \mathfrak{P}_2^3$ oder $\sim \mathfrak{P}_1\ \mathfrak{P}_2$ oder $\sim \mathfrak{P}_1\ \mathfrak{P}_2\ \mathfrak{P}_3\ \mathfrak{P}_1'\ \mathfrak{P}_2'\ \mathfrak{P}_3'$
$p = 3n - 1$	$p \sim \mathfrak{p}$	$p \sim \mathfrak{P}_1\ \mathfrak{P}_2\ \mathfrak{P}_3$ oder $\mathfrak{P}$
$p = 3$	$p \sim \mathfrak{p}^2$	$p \sim \mathfrak{P}_1^6$ oder $\sim \mathfrak{P}_1^2\ \mathfrak{P}_2^2\ \mathfrak{P}_3^2$ oder $\sim \mathfrak{P}^2$

Es soll nun kurz auf den Zusammenhang zwischen dem Hensel'schen reduzierten Legendre'schen Symbol und dem Symbol von Hilbert eingegangen werden, indem der Zusammenhang zwischen dem red. Legendr. Symbol $R\left\{\frac{A}{\mathfrak{p}}\right\}$ und dem Eisenstein'schen Symbol $\left[\frac{A}{\mathfrak{p}}\right]$ festgestellt wird. Ich betrachte zuerst den Fall $\mathfrak{p} \gtrless 3$.

Dazu müssen wir noch näher darauf eingehen, welche Primteiler $\mathfrak{p}$ für $\mathfrak{p} \gtrless 3$ Diskriminantenteiler sind. Darüber gibt der Satz (vgl. Zahlbericht S. 393) Auskunft: Geht eine von $\mathfrak{l} \sim \lambda$ verschiedene Primzahl $\mathfrak{p}$ des Kreiskörpers K (ξ) der $l$ten Einheitswurzeln in A genau zur $e$ten Potenz auf, so enthält, wenn der Exponent e zu l prim ist, die Relativdiskriminante des Kummer'schen Körpers vom Grade $l\,(l-1)$ inbezug auf K (ξ) genau die $l - 1^{te}$ Potenz von $\mathfrak{p}$ als Faktor. Ist der Exponent e dagegen ein Vielfaches von l, so fällt diese Relativdiskriminante prim zu $\mathfrak{p}$ aus.

In unserem Falle heißt das mit anderen Worten, daß die Relativdiskriminante genau die Quadrate aller von $\mathfrak{l} \sim \sqrt{-3}$ verschiedenen in A aufgehenden Primzahlen $\mathfrak{p}$ enthält. Wir können also sagen:

Ist $(3, \mathfrak{p}) = 1$, dann ist $\mathfrak{p}$ dann und nur dann Diskriminantenteiler, wenn es ein Teiler von A ist.

Hilbert gibt (Zahlbericht S. 397) die Primteilerzerlegung für den Fall $\mathfrak{p} \gtrless 3$ an durch Einführung eines Symbols, das eine Erweiterung des Eisenstein'schen Symbols ist, und zwar durch folgende Definition:

Unter dem Symbol $\left[\frac{A}{\mathfrak{p}}\right]$ verstehen wir die folgenden vier in K (ϱ) ganzen Zahlen 0, 1, ϱ, ϱ^2 je nachdem wie $\left[\frac{A}{\mathfrak{p}}\right] \equiv A^{\frac{n(\mathfrak{p})-1}{3}} \bmod \mathfrak{p}$ ausfällt.

Das Symbol hat dann und nur dann den Wert Null, wenn die Relativdiskriminante durch $\mathfrak{p}$ teilbar ist. Ist A prim zu $\mathfrak{p}$, so wird daher das Symbol $\left[\frac{A}{\mathfrak{p}}\right]$ stets einen der Werte 1, ϱ, ϱ^2 besitzen.

Ich setze A als kubischen Kern voraus und zeige, daß unter der Voraussetzung $(A, \mathfrak{p}) = 1$ die Bestimmung des reduz. Legendre'schen Symbols mit der Berechnung des Eisenstein'schen Symbols zusammenfällt. Denke ich mir A multiplikativ dargestellt, so folgt

$$A \equiv w^{\beta} \bmod \mathfrak{p}$$

$\beta < 3$, da A als Kernzahl angenommen ist,

und daraus $A^{\frac{n(\mathfrak{p})-1}{3}} \equiv w^{\beta\frac{n(\mathfrak{p})-1}{3}} \bmod \mathfrak{p}$.

Es ist $A^{\frac{n(\mathfrak{p})-1}{3}} \equiv \left[\frac{A}{\mathfrak{p}}\right] = \varrho^k \bmod \mathfrak{p}$, wo $k = 0, 1, 2$ ist.

π-adisch gesprochen ist $\varrho \equiv w^{\frac{n(\mathfrak{p})-1}{3}} \bmod \mathfrak{p}$ also

$$w^{\frac{n(\mathfrak{p})-1}{3}\beta} \equiv w^{\frac{n(\mathfrak{p})-1}{3}k}$$

$w^{\frac{p^f-1}{3}} = \varrho$ ist primitive dritte Einheitswurzel. Die Kongruenz besteht dann und nur dann, wenn auch Gleichheit besteht, also ist $\varrho^{\beta-k} = 1$ d. h. aber $\beta = k$. Dem-

nach ist $R\left\{\frac{A}{p}\right\} = \varrho^{\beta} = \varrho^{k} = \left[\frac{A}{p}\right]$. Ich betrachte jetzt den Fall $p \gtrless 3$, wo p Diskriminantenteiler, also Teiler von A ist.

$$R\left\{\frac{A}{p}\right\} = \varrho^{a}, \text{ wenn } (A, p) = p \text{ ist.}$$

Denn es ist p in A enthalten, also in der reduzierten multiplikativen Darstellung $\alpha > 0$, also ist nach Definition des reduzierten Legendre'schen Symbols dieses gleich ϱ^{a}.

Wir gehen nun zum Fall $p = 3$ über. Wir fragen so: Wann nimmt für $(3, p) = p$ das reduzierte Legendre sche Symbol einen von ϱ^{a} verschiedenen Wert an?

I. Es ist dann und nur dann $R\left\{\frac{A}{p}\right\} = 1$ wenn A dritter Potenzrest ist und dann und nur dann ist auch $\left[\frac{A}{p}\right] = 1$, also $R\left\{\frac{A}{p}\right\} = \left[\frac{A}{p}\right]$.

II. Es ist $R\left\{\frac{A}{p}\right\} = \varrho^{b}$, dann und nur dann, wenn (1) $(A, p) = 1$ und (2) $A \equiv 1 \bmod p^3$, $A \not\equiv 1 \bmod p^4$ ist. (Vgl. Fall III_c im Anfange des Kapitels).

Da wir so die notwendigen und hinreichenden Bedingungen dafür kennen, daß $R\left\{\frac{A}{p}\right\} = 1$ bezw. ϱ^{b} ist, ist auch der Fall $R\left\{\frac{A}{p}\right\} = \varrho^{a}$ erledigt. Zusammenfassend können wir also sagen:

Satz 1. Ist $p \gtrless 3$, dann nimmt das reduzierte Legendre'sche Symbol $R\left\{\frac{A}{p}\right\}$ den Wert 1 an, wenn das

Eisenstein'sche Symbol $\left[\frac{A}{\mathfrak{p}}\right] = 1$,

den Wert ϱ^a, wenn $\left[\frac{A}{\mathfrak{p}}\right] = 0$,

den Wert ϱ^b, wenn $\left[\frac{A}{\mathfrak{p}}\right] \not\equiv 1$ und $(A, \mathfrak{p}) = 1$ ist.

Satz 2. Ist $p = 3$, dann nimmt das reduzierte Legendre'sche Symbol $R\left\{\frac{A}{\mathfrak{p}}\right\}$ dann und nur dann den Wert 1 an, wenn $(A, \mathfrak{p}) = 1$ und $\left[\frac{A}{\mathfrak{p}}\right] = 1$

den Wert ϱ^b an, wenn $(A, \mathfrak{p}) = 1$ und $A \equiv 1 \bmod \mathfrak{p}^8$
$A \not\equiv 1 \bmod \mathfrak{p}^4$

den Wert ϱ^a in allen anderen Fällen.

Damit ist die Frage nach der Primteilerzerlegung im Kummerschen Körper sechsten Grades vollständig erledigt.

Literatur.

1. *K. Hensel*, Theorie der algebraischen Zahlen, Leipzig 1908.
2. „ „ Eine neue Theorie der algebraischen Zahlen. Mathem. Zeitschrift 2. (1918). (Citiert als H_I.).
3. „ „ Die multiplikative Darstellung der algebraischen Zahlen für den Bereich eines beliebigen Primteilers. Crelle's Journal Bd. 146. (Citiert als H_{II}).
4. „ „ Die Verallgemeinerung des Legendre'schen Symbols für allgem. algebr. Körper. Journal Bd. 147. (Citiert als H_{III}.).
5. „ „ Die Primteilerzerlegung in einem auflösbaren Oberkörper mit einer Anwendung auf Kummersche Körper. Crello's Journal Bd. 151. (Citiert als H_{IV}).
6. *D. Hilbert*, Ueber die Theorie der algebraischen Zahlkörper.
7. *L. Sapolsky*, Ueber die Theorie der relativ-Abel'schen-cubischen Zahlkörper.

Lebenslauf.

Am 27. November 1898 wurde ich, *Aloys Herrmann*, zu Bildstock, Kreis Saarbrücken (Rheinprovinz) als Sohn des Kgl. Betriebsleiters *Jacob Herrmann* geboren. Ich bin katholischer Konfession. Am 22. März 1917 bestand ich an der Oberrealschule zu Saarbrücken die Reifeprüfung und war vom 27. April 1917 bis 18. Dezember 1919 an der Universität Bonn als Studierender der Mathematik und Naturwissenschaften immatrikuliert. 1918 mußte ich meine Studienzeit unterbrechen, da ich in den Heeresdienst eintrat. Seit 21. Januar 1920 studierte ich an der Universität Marburg und wurde am 19. November 1923 exmatrikuliert.

Meine hauptsächlichsten Lehrer waren
in Bonn die Herren Professoren:

Anschütz, H. Beck, H. Hahn, Kayser, Study,

in Marburg die Herren Professoren:

v. Auwers, A. Fränkel, K. Hensel, E. Neumann, F. A. Schulze.

Ihnen allen, insbesondere Herrn Geh. Reg.-Rat Prof. Dr. *Hensel*, sei auch an dieser Stelle mein tiefempfundener Dank ausgesprochen.